ZINĀŠANU BĀZES RAKSTS

Password Vault, pārlūkprogrammu paroļu pārvaldnieki un uzņēmumu paroļu pārvaldnieki: ko izvēlēties

2026 © Vitextra SIA. Visas tiesības paturētas.

Atruna

Šīs atrunas izpratnē:

- **Uzņēmums** (šajā Atrunā – "Uzņēmums", "Mēs", "Mums" vai "Mūsu") ir SIA Vitextra, LV-1009, Rīga, Matīsa iela 61 – 25;
- **Dokuments** attiecas uz zināšanu bāzes rakstu;
- **Jūs** nozīmē fizisku personu, kura piekļūst Dokumentam, vai uzņēmumu, vai citu juridisku personu, kuras vārdā šī fiziskā persona piekļūst Dokumentam vai izmanto to, atkarībā no situācijas;
- **Tīmekļvietne** attiecas uz Vitextra un ir pieejama https://vitextra.com.

Atruna

Dokumentā iekļautā informācija ir paredzēta tikai vispārējai zināšanai.

Uzņēmums neuzņemas atbildību par kļūdām vai izlaidumiem Dokumenta saturā.

Uzņēmums nekādā gadījumā nav atbildīgs par īpašiem, tiešiem, netiešiem, izrietošiem vai nejaušiem zaudējumiem vai jebkādiem citiem zaudējumiem, neatkarīgi no tā, vai tie izriet no līgumā paredzētas darbības, radušies nolaidības vai citu neatļautu darbību dēļ, kas ir radušās no Dokumenta satura izmantošanas vai saistībā ar to. Uzņēmums patur tiesības jebkurā laikā un bez iepriekšēja brīdinājuma papildināt, svītrot vai grozīt Dokumenta saturu.

Atruna par kļūdām un izlaidumiem

Dokumentā sniegtā informācija ir tikai vispārīgas norādes par interešu jautājumiem. Tāpēc kļūdas var rasties pat tad, ja Uzņēmums veic visus piesardzības pasākumus, lai nodrošinātu, ka Dokumenta saturs ir aktuāls un precīzs. Turklāt, ņemot vērā likumu un noteikumu mainīgo dabu, dokumentā iekļautajā informācijā var būt kavējumi, izlaidumi vai neprecizitātes.

Uzņēmums nav atbildīgs par kļūdām vai izlaidumiem, kā arī par rezultātiem, kas ir iegūti, izmantojot šo informāciju.

Atruna par godprātīgu izmantošanu

Uzņēmums var izmantot ar autortiesībām aizsargātu materiālu, ko autortiesību īpašnieks nav skaidri atļāvis. Uzņēmums nodrošina šāda materiāla pieejamību kritikas, komentāru, jaunumu izziņošanas, mācību, zinātniskā darba vai pētniecības nolūkos.

Uzņēmums uzskata, ka tas ir "godprātīgs" šāda ar autortiesībām aizsargāta materiāla izmantojums, kā ir noteikts ASV Autortiesību likuma 107. pantā.

Ja vēlaties izmantot ar autortiesībām aizsargātu materiālu no Dokumenta saviem mērķiem, kas pārsniedz godprātīgu izmantošanu, ir jāsaņem atļauja no autortiesību īpašnieka.

Atruna "Lietošana uz savu risku"

Visa informācija dokumentā tiek sniegta "tāda, kāda tā ir", bez jebkādām pilnīguma, precizitātes, savlaicīguma vai šīs informācijas izmantošanas rezultātā iegūto rezultātu garantijām, kā arī bez jebkādām garantijām, skaidri izteiktām vai netiešām, tostarp, bet ne tikai, bez garantijām par veiktspēju, komerciālo izmantojamību un piemērotību konkrētam mērķim.

Uzņēmums neuzņemas atbildību attiecībā pret Jums vai kādu citu par pieņemto lēmumu vai rīcību, kas pamatojas uz Pakalpojumā sniegto informāciju, vai par izrietošiem, īpašiem vai līdzīgiem zaudējumiem, pat ja Jums ir paziņots par šādu zaudējumu iespējamību.

Sazinieties ar mums

Ja par šo atrunu rodas jautājumi, sazinieties ar Mums pa e-pastu support@vitextra.com.

Satura rādītājs

Pārskats 4

Īsumā par Password Vault 4

Salīdzinājums īsumā 4

Kad Password Vault ir piemērots 6

Kad pārlūkprogrammas paroļu pārvaldnieks ir piemērots 6

Kad uzņēmuma paroļu pārvaldnieks ir piemērots 7

Rīku lietošana līdztekus 7

Jautājumi, kas jāuzdod pirms lēmuma pieņemšanas 7

Pārskats

Organizācijas, kas vēlas, lai darbinieki pārstātu glabāt paroles izklājlapās un piezīmēs, parasti apsver trīs rīku veidus:

- **Pārlūkprogrammu paroļu pārvaldnieki** — tīmekļa pārlūkprogrammās iebūvētā paroļu krātuve, kas saglabā akreditācijas datus, kad lietotājs pierakstās tīmekļa vietnēs.
- **Uzņēmumu paroļu pārvaldnieki** — specializēti produkti, parasti ar savu pakalpojumu, klientu lietotnēm un pārlūkprogrammu paplašinājumiem, kas paredzēti akreditācijas datu pārvaldībai visā organizācijā.
- **Password Vault** — Vitextra SharePoint Framework tīmekļa daļa, kas katram darbiniekam nodrošina vienkāršu personisku glabātuvi pakalpojumā Microsoft 365 (SharePoint Online un Microsoft Teams).

Šie rīki risina dažādas problēmas. Šajā rakstā aprakstītas katras kategorijas vispārīgās īpašības, lai jūs varētu izlemt, kura no tām atbilst konkrētai vajadzībai. Atsevišķi produkti vienas kategorijas ietvaros atšķiras, tāpēc pārbaudiet jebkura apsvērtā produkta īpatnības atbilstoši savām prasībām.

Īsumā par Password Vault

Password Vault glabā katra lietotāja ierakstus šifrētā veidā failā šī lietotāja OneDrive un rāda tos tīmekļa daļā SharePoint lapā vai pakalpojumā Teams. Piekļuvi tīmekļa daļā aizsargā 4 ciparu PIN kods, no kura tiek atvasināta šifrēšanas atslēga; kamēr glabātuve ir bloķēta, ieraksti netiek rādīti, un pēc 5 minūtēm bez darbībām tā tiek bloķēta automātiski. Tā kā PIN kodam ir tikai 4 cipari, faila pirmā aizsardzības līnija joprojām ir piekļuves kontrole OneDrive. Tajā ir paroļu ģenerators, stipruma indikators, mapes, atzīmes, izlase un meklēšana. Sīkāku informāciju skatiet rakstā KB10437. Password Vault. Risinājuma pārskats.

Tikpat svarīgi ir tas, ko tas **nedara**:

- nav pieteikšanās veidlapu automātiskās aizpildes un pārlūkprogrammas paplašinājuma — akreditācijas dati tiek kopēti ar pogu **Kopēt starpliktuvē**;
- nav ierakstu koplietošanas un komandu glabātuvju;
- nav administrēšanas konsoles un aizmirsta PIN koda atkopšanas — pēc 5 nepareiziem PIN kodiem vienīgā iespēja ir atiestatīt glabātuvi, kas izdzēš visus ierakstus;
- nav eksporta vai importa.

Salīdzinājums īsumā

Kolonna Password Vault apraksta produktu; pārējās divas kolonnas apraksta to, kas ir

raksturīgs kategorijai.

Aspekts	Password Vault	Pārlūkprogrammu paroļu pārvaldnieki (parasti)	Uzņēmumu paroļu pārvaldnieki (parasti)
Mērķis	Darbinieka personiskie akreditācijas dati pakalpojumā Microsoft 365	Personiskas ērtības pārlūkošanas laikā	Akreditācijas datu pārvaldība visā organizācijā
Kur tiek glabāti dati	Šifrēts fails paša lietotāja OneDrive	Pārlūkprogrammas profilā, bieži sinhronizēti ar pārlūkprogrammas izstrādātāja kontu	Produkta paša pakalpojumā vai organizācijas uzturētā infrastruktūrā
Piekļuve	SharePoint lapa vai Microsoft Teams, ar darba kontu un 4 ciparu PIN kodu	Pārlūkprogramma, kurā ir pierakstīts profils	Produkta klientu lietotnes, pārlūkprogrammu paplašinājumi un tīmekļa piekļuve
Pieteikšanās veidlapu automātiskā aizpilde	Nē	Jā	Parasti jā
Koplietošana ar kolēģiem	Nē	Ierobežota vai nav darba kontekstā	Parasti jā, ar koplietotām mapēm vai glabātuvēm
Administrēšana, politikas, audits	Nē; tikai izvietošana un Graph atļauja	Atkarīgs no pārlūkprogrammas pārvaldības iespējām	Parasti plašas
Zaudētas piekļuves atkopšana	Nav; atiestatīšana izdzēš glabātuvi	Atkarīgs no pārlūkprogrammas konta	Parasti piedāvā atkopšanas iespējas

Aspekts	Password Vault	Pārlūkprogrammu paroļu pārvaldnieki (parasti)	Uzņēmumu paroļu pārvaldnieki (parasti)
			administratoriem vai lietotājiem
Izvietošana	Viena SPFx pakotne un viena Graph atļauja; bez papildu klienta programmatūras	Jau ir pārlūkprogrammā	Atsevišķs produkts, kas jāievieš, jākonfigurē un jālicencē katram lietotājam
Tipiskais izmaksu modelis	Licence vienam nomniekam	Iekļauts pārlūkprogrammā	Parasti abonements katram lietotājam

Kad Password Vault ir piemērots

- Darbiniekiem ir nepieciešama vieta **saviem** darba akreditācijas datiem — piegādātāju portāliem, partneru ekstranetiem, testa sistēmām, ierīču konsolēm —, un organizācija vēlas, lai šī vieta būtu pakalpojumā Microsoft 365, nevis personiskos rīkos vai failos.
- Organizācija dod priekšroku tam, lai dati paliktu **tās pašas nomniekā** (katra lietotāja OneDrive), nevis pie papildu trešās puses pakalpojuma.
- Vienkāršs rīks, kas darbojas SharePoint lapā un pakalpojumā Teams bez paplašinājumu vai klienta programmatūras instalēšanas, ir svarīgāks par automātisko aizpildi.
- Akreditācijas dati netiek koplietoti, un to zaudēšana, ja PIN kods ir aizmirsts, ir pieņemama, jo tos var atjaunot avota sistēmā (piemēram, izmantojot paša pakalpojuma procesu „aizmirsu paroli”).

Kad pārlūkprogrammas paroļu pārvaldnieks ir piemērots

- Galvenā vajadzība ir ērtības: paroļu saglabāšana un automātiska aizpilde tīmekļa vietnēm pārlūkošanas laikā.
- Lietotāji galvenokārt strādā vienā pārlūkprogrammā, un organizācijas politika atļauj tajā glabāt darba akreditācijas datus.

Ņemiet vērā, ka pārlūkprogrammas paroļu pārvaldnieks glabā akreditācijas datus pārlūkprogrammas profilā, tāpēc tas, kas ir pieejams, ir atkarīgs no pārlūkprogrammas un konta, ar kuru lietotājs ir pierakstījies, kā arī no tā, kā organizācija pārvalda

pārlūkprogrammas.

Kad uzņēmuma paroļu pārvaldnieks ir piemērots

- Akreditācijas dati ir **jākoplieto** komandās, piemēram, pakalpojumu konti vai koplietotas pastkastes.
- Organizācijai ir nepieciešamas centralizētas **politikas, audita žurnāli, piekļuves pārskatīšana un atkopšanas** procedūras.
- Ir jāpārvalda **augstu privilēģiju** administratoru konti — bieži kopā ar privileģētās piekļuves pārvaldību.
- Ir nepieciešama automātiskā aizpilde dažādās pārlūkprogrammās, darbvirsmas un mobilajās lietotnēs.

Šīs iespējas nozīmē atsevišķu produktu, kas jāizvieto, jākonfigurē, jāapmāca tajā lietotāji un jālicencē, parasti katram lietotājam.

Brīdinājums!

Password Vault ir paredzēts personiskiem akreditācijas datiem. Tas neaizstāj risinājumu, kas pārvalda koplietotus vai augstu privilēģiju kontus. Šādiem kontiem ievērojiet savas organizācijas drošības politiku.

Rīku lietošana līdztekus

Kategorijas viena otru neizslēdz. Organizācija var izmantot uzņēmuma paroļu pārvaldnieku IT un koplietotajiem kontiem un piedāvāt Password Vault visiem darbiniekiem kā vienkāršu personisku vietu pārējiem darba akreditācijas datiem — vai atļaut glabāšanu pārlūkprogrammā zema riska tīmekļa vietnēm. Svarīga ir skaidra politika, kurā noteikts, kurš akreditācijas datu veids kur jāglabā.

Piezīme

Password Vault nav importa vai eksporta, tāpēc ierakstu pārvietošana uz to vai no tā nozīmē to pievienošanu pa vienam. Izdariet izvēli, pirms darbinieki sāk aizpildīt savas glabātuves.

Jautājumi, kas jāuzdod pirms lēmuma pieņemšanas

1 Vai akreditācijas dati ir jākoplieto, vai tie ir stingri personiski?
2 Vai ir nepieciešama pieteikšanās veidlapu automātiskā aizpilde?
3 Kur drīkst glabāt šifrētos datus — jūsu Microsoft 365 nomniekā, pārlūkprogrammas

izstrādātāja kontā vai trešās puses pakalpojumā?

4 Vai jums ir nepieciešama administratīva atkopšana, politikas un audits?

5 Ko jūs varat izvietot: SPFx tīmekļa daļu vai klienta programmatūru un paplašinājumus katrā ierīcē?

6 Kas notiek ar akreditācijas datiem, ja lietotājs zaudē piekļuvi, — vai tos var atjaunot avota sistēmā?

Padoms

Lai uzzinātu, kā Password Vault aizsargā datus un kas tiem var piekļūt, izlasiet rakstus KB10452. Kā Password Vault aizsargā jūsu datus: šifrēšana, PIN kods un glabāšana un KB10456. Password Vault: kas var redzēt jūsu paroles. Lai to izmēģinātu, skatiet rakstu KB10438. Kā pievienot Password Vault tīmekļa daļu lapai un izveidot savu glabātuvi.